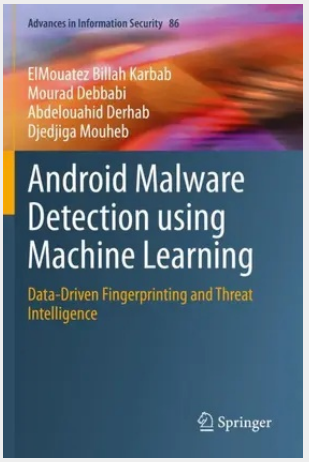
Karbab / Debbabi / Derhab

Android Malware Detection using Machine Learning

Data-Driven Fingerprinting and Threat Intelligence



181,89 €
169,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783030746667
Medium: Buch
ISBN: 978-3-030-74666-7
Verlag: Springer
Erscheinungstermin: 12.07.2022
Sprache(n): Englisch
Auflage: 1. Auflage 2021
Serie: Advances in Information Security
Produktform: Kartoniert
Gewicht: 335 g
Seiten: 202
Format (B x H): 155 x 235 mm

The authors develop a malware fingerprinting framework to cover accurate android malware detection and family attribution in this book. The authors emphasize the following: (1) the scalability over a large malware corpus; (2) the resiliency to common obfuscation techniques; (3) the portability over different platforms and architectures. First, the authors propose an approximate fingerprinting technique for android packaging that captures the underlying static structure of the android applications in the context of bulk and offline detection at the app-market level. This book proposes a malware clustering framework to perform malware clustering by building and partitioning the similarity network of malicious applications on top of this fingerprinting technique. Second, the authors propose an approximate fingerprinting technique that leverages dynamic analysis and natural language processing techniques to generate Android malware behavior reports. Basedon this fingerprinting technique, the authors propose a portable malware detection framework employing machine learning classification. Third, the authors design an automatic framework to produce intelligence about the underlying malicious cyber-infrastructures of Android malware. The authors then leverage graph analysis techniques to generate relevant intelligence to identify the threat effects of malicious Internet activity associated with android malware.
The authors elaborate on an effective android malware detection system, in the online detection context at the mobile device level. It is suitable for deployment on mobile devices, using machine learning classification on method call sequences. Also, it is resilient to common code obfuscation techniques and adaptive to operating systems and malware change overtime, using natural language processing and deep learning techniques.
Researchers working in mobile and network security, machine learning and pattern recognition will find this book useful as a reference. Advanced-level students studying computer science within these topic areas will purchase this book as well.

The authors develop a malware fingerprinting framework to cover accurate android malware detection and family attribution in this book. The authors emphasize the following: (1) the scalability over a large malware corpus; (2) the resiliency to common obfuscation techniques; (3) the portability over different platforms and architectures. First, the authors propose an approximate fingerprinting technique for android packaging that captures the underlying static structure of the android applications in the context of bulk and offline detection at the app-market level. This book proposes a malware clustering framework to perform malware clustering by building and partitioning the similarity network of malicious applications on top of this fingerprinting technique. Second, the authors propose an approximate fingerprinting technique that leverages dynamic analysis and natural language processing techniques to generate Android malware behavior reports. Basedon this fingerprinting technique, the authors propose a portable malware detection framework employing machine learning classification. Third, the authors design an automatic framework to produce intelligence about the underlying malicious cyber-infrastructures of Android malware. The authors then leverage graph analysis techniques to generate relevant intelligence to identify the threat effects of malicious Internet activity associated with android malware.
The authors elaborate on an effective android malware detection system, in the online detection context at the mobile device level. It is suitable for deployment on mobile devices, using machine learning classification on method call sequences. Also, it is resilient to common code obfuscation techniques and adaptive to operating systems and malware change overtime, using natural language processing and deep learning techniques.
Researchers working in mobile and network security, machine learning and pattern recognition will find this book useful as a reference. Advanced-level students studying computer science within these topic areas will purchase this book as well.

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)